**3GPP TSG-SA3 Meeting #124 S3-253845-r1**

**Wuhan, China, 13 – 17 October 2025**

**Source: Samsung**

**Title: Pseudo-CR on SUPI Concealment using hybrid method**

**Document for: Approval**

**Agenda item: 5.2.1**

**Spec: 3GPP TR 33.703**

**Version: v0.1.0**

**Work Item: FS\_CryptoPQC**

**Comments**

This pCR provides SUPI concealment solution using hybrid method.

\* \* \* First Change \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[xx] 3GPP TR 33.938: "3GPP Cryptographic Inventory (Release 19)"

[yy] 3GPP TS 33.501: "Security architecture and procedures for 5G system (Release 19)".

[zz] 3GPP TS 23.003: "Numbering, addressing and identification".

\* \* \* Next Change \* \* \* \*

### 7.2 Solutions

Editor’s Note: This clause contains solutions to update 3GPP defined security protocols (for example SUCI calculation) to use the appropriate PQC algorithm, if those protocols are not expected to be updated by other SDOs to use PQC algorithms.

### 7.2.X Solutions to Protocol #X: SUCI calculations

Editor’s Note: If only SUCI calculation is considered, this subclause may be removed. If other protocol, e.g. MIKEY-SAKKE is studied, this subclause is used for each of such protocol identified.

#### 7.2.X.Y Solution #Y to Protocol #X: SUPI Concealment using hybrid method

##### 7.2.X.Y.1 Introduction

Replacing classical cryptography with PQC algorithms at an early stage carries an inherent risk as a first time widespread deployment and more rigorous testing of PQC algorithms may be needed. So it will be beneficial to have it integrated with classical asymmetric cryptography based security mechanisms via a hybrid approach, where both classical asymmetric algorithms and post-quantum algorithms coexist. In case vulnerabilities are found in either type of algorithm, the presence of both classical and post-quantum algorithms in a hybrid setup reduces the impact of potential breaches, providing additional resilience to the overall cryptography. The hybrid method described here is applying PQC-based key encapsulation mechanism (KEM) to protect final output which is generated via ECIES.

##### 7.2.X.Y.2 Solution details

##### 7.2.X.Y.2.1 Processing on UE side

The processing on UE side is done as follows.



Figure 7.2.X.Y.2.1-1: SUCI generation using hybrid method at UE

1. UE generates a *final output\_ECC* using ECIES as described in Annex C.3.2 in TS 33.501 [yy], where the *final output\_ECC* is Eph. EC public key||ciphertext||MAC tag.

2. UE generates an ephemeral shared key (KPQC) and an encrypted PQC shared key based on a PQC-based public key associated with the home network.

3. UE generates ephemeral symmetric encryption key and ephemeral MAC key using a KDF function and KPQC.

4. UE protects the *final output\_ECC* using the encryption key and the MAC key. The final output is the concatenation of encrypted PQC shared key, ciphertext (i.e., Enc(Eph EC public key||ciphertext||MAC)), and MACtag value.

**Figure 7.2.X.Y.2.1-1** defines the scheme output (i.e., the final output in step 4) as a result of the above steps, as defined in TS 23.003 [zz].



Figure 7.2.X.Y.2.1-2: Scheme output based on hybrid method

Note: Ciphertext output from PQC key encapsulation is referred to as encrypted PQC shared key as there is another ciphertext value from step 3 of symmetric encryption, to avoid confusion.

##### 7.2.X.Y.2.2 Processing on home network side

The processing on home network (HN) side is done as follows.



Figure 7.2.X.Y.2-3: Decryption based on hybrid method at home network

1. Home network (HN) decapsulates the encrypted PQC shared key to derive the ephemeral shared key (KPQC).

2. HN generates ephemeral symmetric encryption key and ephemeral MAC key using a KDF function and KPQC.

3. HN verifies the MAC and decrypts the ciphertext to derive the *final output\_ECC*, using the MAC key and encryption key respectively.

4. HN obtain the plaintext block (i.e., UE ID) using ECIES as described in Annex C.3.3 in TS 33.501 [yy].

Note: Ciphertext input to PQC key decapsulation is referred to as encrypted PQC shared key as there is another ciphertext value from step 3 of symmetric decryption, to avoid confusion.Editor’s note: performances due to PQC operations performed after ECIES operations are FFS.

##### 7.2.X.Y.3 Evaluation

TBD

\* \* \* End of Changes \* \* \* \*